

**EXHIBIT A**

E-FILED  
1/23/2024 10:32 PM  
Clerk of Court  
Superior Court of CA,  
County of Santa Clara  
24CV429673  
Reviewed By: A. Montes

Potter Handy, LLP  
Mark Potter, Esq., SBN 166317  
Barry Walker, Esq., SBN 195947  
Jim Treglio, Esq., SBN 228077  
Christina Carson, Esq. SBN 280048  
Tehniat Zaman, Esq. SBN 321557  
Mail: 100 Pine St., Ste. 1250  
San Francisco, CA 94111  
(415) 534-1911; (888) 422-5191 fax  
[23andMeIL@potterhandy.com](mailto:23andMeIL@potterhandy.com)  
Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA  
SANTA CLARA COUNTY

**TRISHA WILKUS; RYAN FOWLER;  
ARTURO GONZALEZ; SARAH  
SCHULTZ; CASSANDRA  
SALGADO; MELANIE DIMUZIO;  
DARLENE EBY; SANDY  
LANDVICK; DALIA RAMAHI;  
PATTY ZINK; KATHARINA  
RYASATI; STEVE TEMKIN; AND  
NICOLE CASSIDY,**

Plaintiff,

v.

**23ANDME, INC.,**

Defendant.

Case No. 24CV429673

**COMPLAINT FOR CIVIL  
DAMAGES AND INJUNCTIVE  
RELIEF**

- 1. Illinois Genetic Information Privacy Act**
- 2. Negligence**
- 3. Breach Of Actual and Implied Contract**
- 4. Invasion Of Privacy – Intrusion Upon Seclusion**
- 5. Unjust Enrichment**

**JURY TRIAL DEMANDED**

**COMPLAINT**

Plaintiffs Trisha Wilkus; Ryan Fowler; Arturo Gonzalez; Sarah Schultz;  
Cassandra Salgado; Melanie DiMuzio; Darlene Eby; Sandy Landvick; Dalia Ramahi;  
Patty Zink; Katharina Ryasati; Steve Temkin; and Nicole Cassidy, (collectively

“Plaintiffs”) allege against Defendant 23andMe, Inc. (“23andMe” or “Defendant”) as follows:

**SUMMARY:**

1. Defendant is a genomic and biotechnology company that looks at an individual’s genome for the purpose of creating unique, personalized genetic reports on ancestral origins, personal genetic health risks, chances of passing on carrier conditions, and pharmacogenetics.<sup>1</sup>
2. To take advantage of Defendant’s services, customers had to provide sensitive personal, genetic, and biological information. To gain the trust of potential customers Defendant expressly advertised the importance of security as “Privacy is in our DNA”.
3. On or about October 6, 2023, Defendant announced, via their website, that unauthorized threat actors had accessed 23andMe accounts and compiled customer profile information (the “Data Breach”).<sup>2</sup>
4. The Data Breach contained millions of individuals’ private identifying information (hereinafter “PII”), including, but not limited to: names, sex, date of birth, usernames, genetic ancestry, profile photos, geographical locations, living biological relatives, and data about individuals’ ethnicity.
5. Plaintiffs are customers of 23andMe that were victims of the Data Breach. Due to the Data Breach, Plaintiffs’ PII was released, stolen, and offered for sale on the dark web.
6. Defendant had a non-delegable duty and responsibility to implement and maintain reasonable security measures to secure, safeguard, and protect the private information that it collected, stored, and maintained for Plaintiffs.
7. Defendant disregarded the rights of Plaintiffs by intentionally, willfully, recklessly, or negligently failing to implement adequate and reasonable measures to ensure that

<sup>1</sup> <https://www.23andme.com/#> (last visited January 9, 2024).

<sup>2</sup> <https://blog.23andme.com/articles/addressing-data-security-concerns>

1 Plaintiffs' PII was safeguarded, failing to take all available steps to prevent  
2 unauthorized disclosure of data, and failing to follow applicable, and appropriate  
3 protocols, policies, and procedures regarding the encryption of data. The Data  
4 Breach was a direct result of Defendant's failure to implement adequate and  
5 reasonable cyber-security procedures and protocols necessary to protect victims'  
6 PII.

7 8. As a result of Defendant's failure to implement adequate data security measures,  
8 Plaintiffs have suffered actual harm in the disclosure of their PII to unknown and  
9 unauthorized third parties. Plaintiffs have suffered injury and ascertainable losses in  
10 the form of the present and imminent threat of fraud and identity theft, loss of the  
11 benefit of their bargain, out-of-pocket expenses, loss of value of their time  
12 reasonably incurred to remedy or mitigate the effects of the attack, and the loss of,  
13 and diminution in, value of their PII. Plaintiffs also remain vulnerable to future  
14 cyberattacks and thefts from the data in Defendant's possession.

15 9. As such, Plaintiffs assert claims for Illinois Genetic Information Privacy Act  
16 (GIPA), 410 ILCS 513 *et seq.*; negligence, breach of implied contract, invasion of  
17 privacy, and unjust enrichment.

18 **JURISDICTION AND VENUE:**  
19

20 10. This Court has subject matter jurisdiction over this action pursuant to Article VI,  
21 section 10 of the California Constitution and Code of Civil Procedure section  
22 410.10

23 11. This Court has personal jurisdiction over Defendant because it is headquartered in  
24 the State of California, county of Santa Clara, and purposefully avails itself of the  
25 laws, protections, and advantages of this State.

26 12. Venue is proper in this Court because Defendant conducts business in this County  
27 and reaped substantial profits from customers in this County. In addition, in its own  
28 Terms of Service, Defendant has agreed "...to submit to the exclusive jurisdiction

of any state or federal court located in Santa Clara County, California (except for small claims court actions which may be brought in the county where you reside), and waive any jurisdictional, venue, or inconvenient forum objections to such courts.” Finally, a substantial part of the acts and conduct charged herein occurred in this County.

### **PARTIES:**

13. Plaintiffs are residents of Illinois who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data Breach.
14. Defendant 23andMe, Inc. is a biotechnology company headquartered in California that collects and analyzes an individual’s genome for the purpose of creating personalized genetic reports directly to consumers.

### **FACTUAL ALLEGATIONS:**

#### ***Defendant collected and stored Plaintiffs’ PII***

15. Defendant collects PII from their customers in the course of doing business.
16. As a condition of receiving Defendant’s services, Plaintiffs were required to entrust Defendant with highly sensitive genetic information, information derived from genetic testing, health information, ancestral origin, and other confidential and sensitive PII. 23andMe then stores that information in its platform.
17. According to the Privacy Statement on 23andMe’s website, the company collects the following categories of customer information:
  - a) Registration Information, including name, user ID, password, date of birth, billing address, shipping address, payment information, account authentication information, and contact information (such as email address and phone number).
  - b) Genetic information, including “[i]nformation regarding your genotype (e.g., the

As, Ts, Cs, and Gs at particular locations in your DNA)” and “the 23andMe genetic data and reports provided to you as part of our Services.”

- c) Sample Information, including “[i]nformation regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with Genetic Information, laboratory values or other data provided through our Services.”
  - d) Self-Reported Information, including “gender, disease conditions, health related information, traits, ethnicity, family history, or anything else you want to provide to us within our Service(s).”
  - e) User Content, including “[i]nformation, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services.”
  - f) Web-Behavior Information, including “[i]nformation on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, location, domains, page views).”
  - g) Biometric Information, including “[c]ertain Self-Reported Information you provide to us or our service providers to verify your identity using biological characteristics.”
18. As part of its advertising, Defendant promises to maintain the confidentiality of Plaintiffs’ PII to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiffs’ PII for non-essential purposes.
19. Defendant’s Privacy Policy states that it “encrypt[s] all sensitive information and conduct[s] regular assessments to identify security vulnerabilities and threats.”<sup>3</sup>

---

<sup>3</sup> <https://www.23andme.com/privacy/>

- 1 20. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' PII,  
2 Defendant assumed legal and equitable duties and knew or should have known that  
3 it was responsible for protecting Plaintiffs' PII from unauthorized disclosure.
- 4 21. Additionally, Defendant had and continues to have obligations created by applicable  
5 state law, reasonable industry standards, common law, and its own assurances and  
6 representations to keep Plaintiffs' PII confidential and to protect such PII from  
7 unauthorized access.
- 8 22. Defendant created the reasonable expectation and mutual understanding with  
9 Plaintiffs that it would comply with its obligations to Plaintiffs' information,  
10 including the PII, confidential and secure from unauthorized access.
- 11 23. Plaintiffs have the utmost privacy interest in the highly sensitive nature of PII, and  
12 would not have been induced to purchase the genetic testing offered by Defendant  
13 had Defendant not included privacy assurances within its advertising.
- 14 24. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied  
15 on Defendant to keep their PII confidential and securely maintained, to use this  
16 information for business purposes only, and to make only authorized disclosures of  
17 this information.

18  
19 ***Data Breach***

- 20 25. On October 6, 2023, Defendant revealed that threat actors were able to access  
21 customer accounts and obtain customers' PII without authorization and consent.
- 22 26. Despite the prevalence of public announcements of data breach and data security  
23 compromises in recent years, Defendant failed to take sufficient steps to protect  
24 Plaintiffs' PII from being compromised.
- 25 27. Upon information and belief, Defendant did not require two-factor authentication to  
26 protect Plaintiffs' PII at the time of the Data Breach.
- 27 28. Upon information and belief, Defendant did not adequately monitor, secure, and/or  
28 encrypt its servers and Plaintiffs' PII.

1 29. Upon information and belief, Defendant could have prevented the Data Breach.

2 30. Upon information and belief, the cyberattack was expressly designed to gain access  
3 to private and confidential data, including Plaintiffs' PII.

4 31. Due to Defendant's inadequate security measures, Plaintiffs now face a present,  
5 immediate, and ongoing risk of fraud and identity theft and must deal with that  
6 threat indefinitely.

7  
8 ***Defendant failed to adequately protect the PII and failed to timely notify Plaintiffs their***  
9 ***data had been compromised***

10 32. On November 6, 2023—one month after it disclosed the breach—23andMe  
11 announced that it was “requiring all customers use a second step of verification to  
12 sign into their account.”

13 33. On information and belief, Defendant did not begin notifying Plaintiffs their  
14 specific PII had been compromised until on or after December 1, 2023.

15 34. On information and belief, Defendant continues to fail to take reasonable and  
16 adequate measure to notify all impacted customers that their PII has been  
17 compromised.

18 35. At all relevant times, Defendant had a duty to exercise reasonable care in obtaining,  
19 retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's  
20 possession from being compromised, lost, stolen, accessed, and misused by  
21 unauthorized persons.

22 36. At all relevant times, Defendant had a duty to properly secure the collected PII,  
23 encrypt and maintain such information using industry standard methods, create and  
24 implement reasonable data security practices and procedures, train its employees,  
25 utilize available technology to defend its systems from invasion, act reasonably to  
26 prevent foreseeable harm to Plaintiffs, and to promptly notify Plaintiffs when  
27 Defendant became aware that Plaintiffs' PII may have been compromised.

28 37. Defendant touted its security and privacy as part of their advertising. Defendant's



duty to use reasonable security measures arose as a result of the Plaintiffs' reasonable reliance on Defendant to secure their highly sensitive personal data. Plaintiffs surrendered the data to obtain Defendant's services under the express condition that Defendant would keep it private and secure. Accordingly, Defendant also has a duty to safeguard their data, independent of any statute.

38. Defendant owed a duty of care to Plaintiffs because they were foreseeable and probable victims of any inadequate data security practices.

### ***Value of the PII***

39. PII are highly valuable for identity thieves and personal information is sold on several underground internet websites for \$40 to \$200<sup>4</sup> per identity.

40. Identity thieves can use PII, such as that of Plaintiffs to perpetrate a variety of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

41. Criminals can also use stolen PII to extort a financial payment by leveraging sensitive healthcare information, for example a sexually transmitted disease or terminal illness, to extort or coerce the victim.

42. Familial relationships and ethnic background can be used to target certain minority groups with threats or even violence.

43. Data breaches involving medical information are more difficult to detect, and take longer to uncover, than normal identity theft. In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief can use private information "to see a doctor, get prescription drugs, buy medical devices, submit

---

<sup>4</sup> Anita George, DIGITAL TRENDS, Your personal data is for sale on the dark web. Here's how much it costs (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

claims with your insurance provider, or get other medical care.”<sup>5</sup> The FTC also warns that if a thief’s health information is mixed with the victim’s it “could affect the medical care [they are] able to get or the health insurance benefits [they are] able to use.”<sup>6</sup>

44. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs. It knew, or should have known, that PII is sought after and valuable target for thieves and that there was a high likelihood this information would be targeted. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

45. Defendant disregarded the rights of Plaintiffs by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs’ PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and/or extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff prompt and accurate notice of the Data Breach.

46. Plaintiffs have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have fear, stress, anxiety and increased concerns for the loss of their privacy and PII being in the hands of criminals.

47. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

---

<sup>5</sup> See What to Know About Medical Identity Theft, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Oct. 2, 2023).

<sup>6</sup> *Id.*

1 48. As a result of the Data Breach, Plaintiffs are at risk and will continue to be at  
2 increased risk of identity theft and fraud for years to come.

3 49. Plaintiffs have a continuing interest in ensuring that their Private Information, which,  
4 upon information and belief, remains backed up in Defendant's possession, is  
5 protected and safeguarded from future breaches.

6 ***Defendant Fails to Comply with FTC Guidelines***

7 50. The Federal Trade Commission ("FTC") has promulgated numerous guides for  
8 businesses which highlight the importance of implementing reasonable data security  
9 practices.

10 51. FTC guidelines note that businesses should protect the personal customer  
11 information that they keep; properly dispose of personal information that is no  
12 longer needed; encrypt information stored on computer networks; understand their  
13 network's vulnerabilities; and implement policies to correct any security problems.

14 52. The guidelines also recommend companies not maintain Private Information longer  
15 than is needed for authorization of a transaction; limit access to sensitive data;  
16 require complex passwords to be used on networks; use industry-tested methods for  
17 security; monitor for suspicious activity on the network; and verify that third-party  
18 service providers have implemented reasonable security measures. Further, it  
19 recommends businesses use an intrusion detection system to expose a breach as  
20 soon as it occurs; monitor all incoming traffic for activity indicating someone is  
21 attempting to hack the system; watch for large amounts of data being transmitted  
22 from the system; and have a response plan ready in the event of a breach.<sup>7</sup>

23 53. The FTC guidelines also form part of the basis of Defendant's duty in this regard.

24 54. Upon information and belief, Defendant was at all times fully aware of its  
25 obligation to protect the PII of its customers, Defendant was also aware of the  
26 significant repercussions that would result from its failure to do so. Accordingly,

27  
28 <sup>7</sup> Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at  
[https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
(last visited Oct. 2, 2023).

1 Defendant's conduct was particularly unreasonable given the nature and amount of  
2 PII it obtained and stored and the foreseeable consequences of the immense  
3 damages that would result to Plaintiffs.

4 ***Injuries and Damages:***

5 55. As a result of the Data Breach, Plaintiffs have all sustained actual injuries and  
6 damages, including: (i) lost or diminished value of their PII; (ii) lost opportunity  
7 costs associated with attempting to mitigate the actual consequences of the Data  
8 Breach, including but not limited to lost time; (iii) lost time spent on activities  
9 remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss  
10 of benefit of the bargain; (vi) the continued and certainly increased risk to their PII;  
11 and (vii) fear, stress, and anxiety.

12 56. The information disclosed in this Data Breach is impossible to change. Plaintiffs  
13 will have to monitor for identity theft and breaches their entire lives. The retail cost  
14 of credit monitoring and identity theft monitoring can cost around \$200 a year per  
15 Plaintiff. This is a reasonable and necessary cost to monitor to protect Plaintiffs  
16 from the risk of identity theft that arose from the Data Breach. This is a future cost  
17 that Plaintiffs would not need to bear but for Defendant's failure to safeguard their  
18 PII.

19  
20 **CLAIMS FOR RELIEF:**

21 **COUNT I: Illinois Genetic Information Privacy Act** (On behalf of all Plaintiffs).

22 57. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this  
23 complaint.

24 58. The Genetic Information Privacy Act (GIPA), 410 Ill. Comp. Stat. Ann. 513 *et seq.*,  
25 covers "[c]onfidentiality of genetic information" and provides in relevant part:  
26 "Except as otherwise provided in this Act, genetic testing and information derived  
27 from genetic testing is confidential and privileged and may be released only to the  
28 individual tested and to persons specifically authorized, in writing in accordance

1 with Section 30, by that individual to receive the information.” 410 Ill. Comp. Stat.  
2 Ann. 513/15(a).

3 59. GIPA incorporates the definition of “genetic information” from 45 C.F.R. §  
4 160.103, which defines the term as “information about” an individual’s “genetic  
5 tests,” “[t]he genetic tests of family members of the individual,” “[t]he  
6 manifestation of a disease or disorder in family members of such individual,” or  
7 “[a]ny request for, or receipt of, genetic services, or participation in clinical research  
8 which includes genetic services, by the individual or any family member of the  
9 individual.”

10 60. GIPA also incorporates the definition of “genetic test” from 45 C.F.R. § 160.103,  
11 which defines the term as “an analysis of human DNA, RNA, chromosomes,  
12 proteins, or metabolites, if the analysis detects genotypes, mutations, or  
13 chromosomal changes.”

14 61. The test performed by 23andMe qualifies as “genetic testing” under GIPA because  
15 it detects, inter alia, genotypes and mutations.

16 62. The information compromised in the breach of 23andMe’s platform included  
17 genetic information, genetic testing, and information derived from such  
18 information. For example, the origin of Plaintiffs’ ancestors, the list of other  
19 23andMe users identified by 23andMe as Plaintiff’s DNA relatives, and the  
20 information on the number of DNA segments Plaintiffs shared with those other  
21 users were all information about, and derived from, the 23andMe genetic test  
22 Plaintiff purchased. Moreover, these results serve as a receipt of genetic services  
23 performed by 23andMe for Plaintiff.

24 63. 23andMe negligently and recklessly released Plaintiff and class members’ genetic  
25 information, PII, and other confidential and highly sensitive PII by failing to  
26 adequately safeguard that information from malicious actors. Considering the  
27 number of data breaches and the sensitivity of the information it possessed,  
28 23andMe was aware or should have been aware of the need to implement robust

1 security measures to protect such information. It consciously refused to do so.

2 64. By negligently and recklessly releasing Plaintiffs' information (including genetic  
3 testing and information derived from genetic testing performed by 23andMe) to  
4 unauthorized parties, as alleged above, 23andMe violated GIPA.

5 65. Accordingly, Plaintiffs are entitled to, and seek, damages of "\$2,500 or actual  
6 damages, whichever is greater," for each negligent violation, or "\$15,000 or actual  
7 damages, whichever is greater," for each intentional or reckless violation, as well as  
8 reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.

9 66. Plaintiffs are also authorized to obtain injunctive relief to prevent future violations.  
10 *Id.*

11  
12 **COUNT II: Negligence** (On behalf of all Plaintiffs).

13 67. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this  
14 complaint.

15 68. At all times herein relevant, Defendant owed Plaintiffs a duty of care, *inter alia*, to  
16 act with reasonable care to secure and safeguard their PII and to use commercially  
17 reasonable methods to do so. Defendant took on this obligation upon accepting and  
18 storing the PII of Plaintiffs in its computer systems and on its networks.

19 69. Defendant knew that the PII was private and confidential and should be protected  
20 and, thus, Defendant owed a duty of care not to subject Plaintiffs to an unreasonable  
21 risk of harm because they were foreseeable and probable victims of any inadequate  
22 security practices.

23 70. Defendant knew, or should have known, of the risks inherent in collecting and  
24 storing PII, the vulnerabilities of its data security systems, and the importance of  
25 adequate security.

26 71. Defendant knew, or should have known, that its data systems and networks did not  
27 adequately safeguard Plaintiffs' PII.

28 72. Only Defendant was in the position to ensure that its systems and protocols were

1 sufficient to protect the PII that Plaintiffs had entrusted to it.

2 73. Because Defendant knew that a breach of its systems could damage thousands of  
3 individuals, including Plaintiffs, Defendant had a duty to adequately protect its data  
4 systems and the PII contained therein.

5 74. Plaintiffs' willingness to entrust Defendant with their PII was predicated on the  
6 understanding that Defendant would take adequate security precautions.

7 75. Moreover, only Defendant had the ability to protect its systems and the PII stored  
8 on them from attack.

9 76. Defendant also had independent duties under state laws that required Defendant to  
10 reasonably safeguard Plaintiffs' PII and promptly notify them about the Data  
11 Breach. These "independent duties" are untethered to any contract between  
12 Defendant and Plaintiffs.

13 77. Defendant breached its general duty of care to Plaintiffs in, but not necessarily  
14 limited to, the following ways:

15 a) By failing to exercise reasonable care in obtaining, retaining, securing,  
16 safeguarding, deleting, and protecting the PII in its possession;

17 b) By failing to protect Plaintiffs' PII using reasonable and adequate  
18 security procedures and systems that were/are compliant with FTC  
19 guidelines and industry-standard practices.

20 c) By failing to implement processes to detect the Data Breach, security  
21 incidents or intrusions,

22 d) By failing to quickly and to timely act on warnings about data  
23 breaches;

24 e) By failing to timely and promptly notify Plaintiff of any data breach,  
25 security incident, or intrusion that affected or may have affected their  
26 PII; and

27 f) By failing to provide adequate supervision and oversight of the PII  
28 with which it was and is entrusted, in spite of the known risk and

foreseeable likelihood of breach and misuse.

78. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

79. To date, Defendant has not provided sufficient information to Plaintiffs regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs.

80. Further, through its failure to provide clear notification of the Data Breach to Plaintiffs, Defendant prevented Plaintiffs from taking meaningful, proactive steps to secure their PII.

81. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the harm suffered, or risk of imminent harm suffered, by Plaintiffs.

82. Defendant's wrongful actions, inactions, and omissions constituted, and continue to constitute, common law negligence.

83. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will suffer injury, including but not limited to:

- a) actual identity theft;
- b) the loss of the opportunity of how their PII is used;
- c) the compromise, publication, and/or theft of their PII;
- d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft;
- f) the continued risk to their PII, which may remain in Defendant's



possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' PII in its continued possession; and

g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs.

84. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**COUNT III: BREACH OF ACTUAL AND IMPLIED CONTRACT** (On behalf of all Plaintiffs)

85. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

86. Defendant specifically advertised a feature of the service they offer is privacy and security.

87. Plaintiffs believed their PII would be stored and remain private and secure as a condition of purchasing Defendant's services. In so doing, Plaintiffs entered into actual and implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs if their data had been breached and compromised or stolen.

88. At the time Defendant acquired the PII of Plaintiffs, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

89. Implicit in the agreements between Plaintiffs and Defendant to provide PII, was the

Defendant's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) retain the PII only under conditions that kept such information secure and confidential, and (e) provide Plaintiffs with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

90. Plaintiffs fully performed their obligations under the actual and implied contracts with Defendant.

91. Defendant breached the actual and implied contracts they made with Plaintiffs by failing to safeguard and protect their personal information, by failing to delete the information that it no longer needed, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

92. As a direct and proximate result of Defendant's above-described breach of actual and implied contract, Plaintiffs have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse; actual identity theft crimes, fraud, and abuse; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; fear, stress, and anxiety; and other economic and non-economic harm.

93. As a direct and proximate result of Defendant's above-described breach of actual and implied contract, Plaintiffs are entitled to recover actual, consequential, and nominal damages to be determined at trial.

**COUNT IV: INVASION OF PRIVACY – INTRUSION UPON SECLUSION** (On behalf of all Plaintiffs)

94. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this

1 complaint.

2 95. Plaintiffs have a legally protected privacy interest in their PII, which is and was  
3 collected, stored and maintained by Defendant, and they are entitled to the  
4 reasonable and adequate protection of their PII against foreseeable unauthorized  
5 access, as occurred with the Data Breach.

6 96. Plaintiffs reasonably expected that Defendant would protect and secure their PII  
7 from unauthorized parties and that their PII would not be accessed, removed, and/or  
8 disclosed to any unauthorized parties or for any improper purpose.

9 97. Defendant intentionally intruded into Plaintiffs' seclusion by disclosing without  
10 permission their PII to a third party. Defendant's acts and omissions giving rise to  
11 the Data Breach were intentional in that the decisions to implement lax security and  
12 failure to timely notice Plaintiffs were undertaken willfully and intentionally.

13 98. By failing to keep Plaintiffs' PII secure, and disclosing PII to unauthorized parties  
14 for unauthorized use, Defendants unlawfully invaded Plaintiffs' privacy right to  
15 seclusion by, inter alia:

16 a) invading their privacy by improperly using their PII obtained for a specific  
17 purpose for another purpose, or disclosing it to unauthorized persons;

18 b) failing to adequately secure their PII from disclosure to unauthorized persons;  
19 and

20 c) enabling the disclosure of their PII without consent.

21 99. This invasion of privacy resulted from Defendant's intentional failure to properly  
22 secure and maintain Plaintiffs' PII, leading to the foreseeable unauthorized access,  
23 removal, and disclosure of this unguarded and private data.

24 100. Plaintiffs' PII is the type of sensitive, personal information that one normally  
25 expects will be protected from exposure by the very entity charged with  
26 safeguarding it. Further, the public has no legitimate concern in Plaintiffs' PII, and  
27 such information is otherwise protected from exposure to the public by various  
28 statutes, regulations and other laws.

1 101. The disclosure of Plaintiffs' PII to unauthorized parties is substantial and  
2 unreasonable enough to be legally cognizable and is highly offensive to a  
3 reasonable person.

4 102. Defendant's willful and reckless conduct that permitted unauthorized access,  
5 removal, and disclosure of Plaintiffs' sensitive PII is such that it would cause  
6 serious mental injury, shame or humiliation to people of ordinary sensibilities.

7 103. The unauthorized access, removal, and disclosure of Plaintiffs' PII was without  
8 their consent, and in violation of various statutes, regulations, and other laws.

9 104. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs  
10 suffered injury and sustained actual losses and damages as alleged herein.

11 105. Plaintiffs alternatively seek an award of nominal damages.  
12

13 **COUNT V: UNJUST ENRICHMENT** (On behalf of Plaintiffs)

14 106. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this  
15 complaint.

16 107. By its wrongful acts and omissions described herein, Defendant has obtained a  
17 benefit by unduly taking advantage of Plaintiffs.

18 108. Defendant, prior to and at the time Plaintiffs entrusted their PII to Defendant,  
19 caused Plaintiffs to reasonably believe that Defendant would keep such PII secure.

20 109. Defendant was aware, or should have been aware, that reasonable consumers would  
21 want their PII secured and would not have contracted with Defendant, directly or  
22 indirectly, had they known that Defendant's information systems were substandard  
23 for that purpose.

24 110. Defendant was also aware that, if the substandard condition of and vulnerabilities in  
25 its information systems were disclosed, it would negatively affect Plaintiffs'  
26 decisions to seek services from Defendant.

27 111. Defendant failed to disclose facts pertaining to its substandard information systems,  
28 defects, and vulnerabilities therein before Plaintiffs made their decisions to make

purchases, engage in commerce therewith, and seek services or information.

112. Defendant denied Plaintiffs the ability to make an informed purchasing decision and took undue advantage of Plaintiffs.

113. Defendant was unjustly enriched at the expense of Plaintiffs, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs; however, Plaintiffs did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

114. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation, or profits it realized from these transactions.

115. Plaintiffs seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs may seek restitution.

**PRAYER:**

Wherefore, Plaintiffs request that this Court award damages and provide relief as follows:

- A. Pursuant to the Illinois Genetic Information Privacy Act, damages of \$2,500 or actual damages, whichever is greater, for each negligent violation, or \$15,000 or actual damages, whichever is greater, for each intentional or reckless violation, as well as reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.
- B. For for all other compensatory damages, statutory damages, punitive damages, restitution, and/or recovery of such relief as permitted by law in kind and amount;
- C. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs;

1 D. For injunctive relief requested by Plaintiff, including but not limited to:

- 2 i. prohibiting Defendant from engaging in the wrongful and unlawful acts  
3 described herein;
- 4 ii. requiring Defendant to protect, including through encryption, all data  
5 collected through the course of business;
- 6 iii. requiring Defendant to delete and purge the PII of Plaintiffs unless  
7 Defendant can provide to the Court reasonable justification for the  
8 retention and use of such information when weighed against the privacy  
9 interests of Plaintiffs;
- 10 iv. requiring Defendant to implement and maintain a comprehensive security  
11 program designed to protect the confidentiality and integrity of Plaintiffs'  
12 PII;
- 13 v. requiring Defendant to engage independent third-party security auditors  
14 and internal personnel to run automated security monitoring, simulated  
15 attacks, penetration tests, and audits on Defendant's systems periodically;
- 16 vi. prohibiting Defendant from maintaining Plaintiffs' PII on a cloud-based  
17 database;
- 18 vii. requiring Defendant to segment data by creating firewalls and access  
19 controls so that, if one area of Defendant's network is compromised,  
20 hackers cannot gain access to other portions of Defendant's systems;
- 21 viii. requiring Defendant to conduct regular database scanning and securing  
22 checks;
- 23 ix. requiring Defendant to establish an information security training program  
24 for all employees, with additional training for employees' responsible for  
25 handling PII;
- 26 x. requiring Defendant to implement a system of tests to assess its respective  
27 employees' knowledge of the education programs discussed in the  
28 preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xi. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

xii. requiring Defendant to meaningfully educate Plaintiffs about the threats they face due to the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

E. for pre- and post-judgment interest on all amounts awarded, at the prevailing legal rate;

F. for an award of attorney's fees, costs, and litigation expenses; and


G. for all other Orders, findings, and determinations identified and sought in this Complaint.

### **JURY DEMAND**

Plaintiffs hereby demand a trial by jury for all issues triable by jury.

Dated:

POTTER HANDY LLP

By:   
Tehniat Zaman, Esq.  
Attorney for Plaintiffs